The Rise of Data Breaches and the Imperative for Database Security

Sean Duca
Enterprise Solutions Architect

AGENDA

- Life's a breach… WITHOUT dedicated database security
- Overcoming Database Security Challenges with McAfee
- McAfee's Database Security
- Demonstration
- Q & A

Databases Contain Your Crown Jewels

Customer Records and PII

- Credit card numbers, account numbers, billing information, authentication data, their data

Employee Information

- Salary, reviews, Tax File Numbers, Bank Details

Financial Data and IP

- Revenue, Receivables, Bill of Materials, Research & Development

Perimeter security still leaves your databases exposed to:

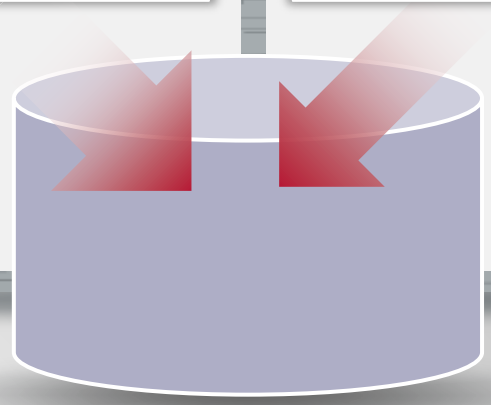
McAfee
An Intel Company

PRIVILEGED USERS (DBA'S, SYS ADMINS, DEVELOPERS) EASILY GO UNDETECTED:

- Abusing permissions
- Audit log tampering
- Leaving backdoors—infrastructure and code
- Hackers often aim to gain privileged status

REGULAR USERS WITHIN THE PERIMETER

- Rogue behavior, unintentional errors, human curiosity
- Network scanning
- Password attacks
- Abusing authorized access
- Privilege elevation



Securing your databases can be very challenging

"I'm **not even sure where all my databases are**,
or how securely they are configured…"

"We have **limited visibility or controls over actual activity in our databases**, especially by privileged users."

"My auditors require logs showing exactly who made changes to certain data, but some of our applications connect directly to the database **so I don't always know who issued commands**."

"Many of our applications are running on top of databases that are **too critical to take down**, or on ones that the DBMS vendor doesn't even release patches for anymore."

McAfee Database Security Solution

Database Vulnerabilities

Patching

Threats and Risks

Compliance

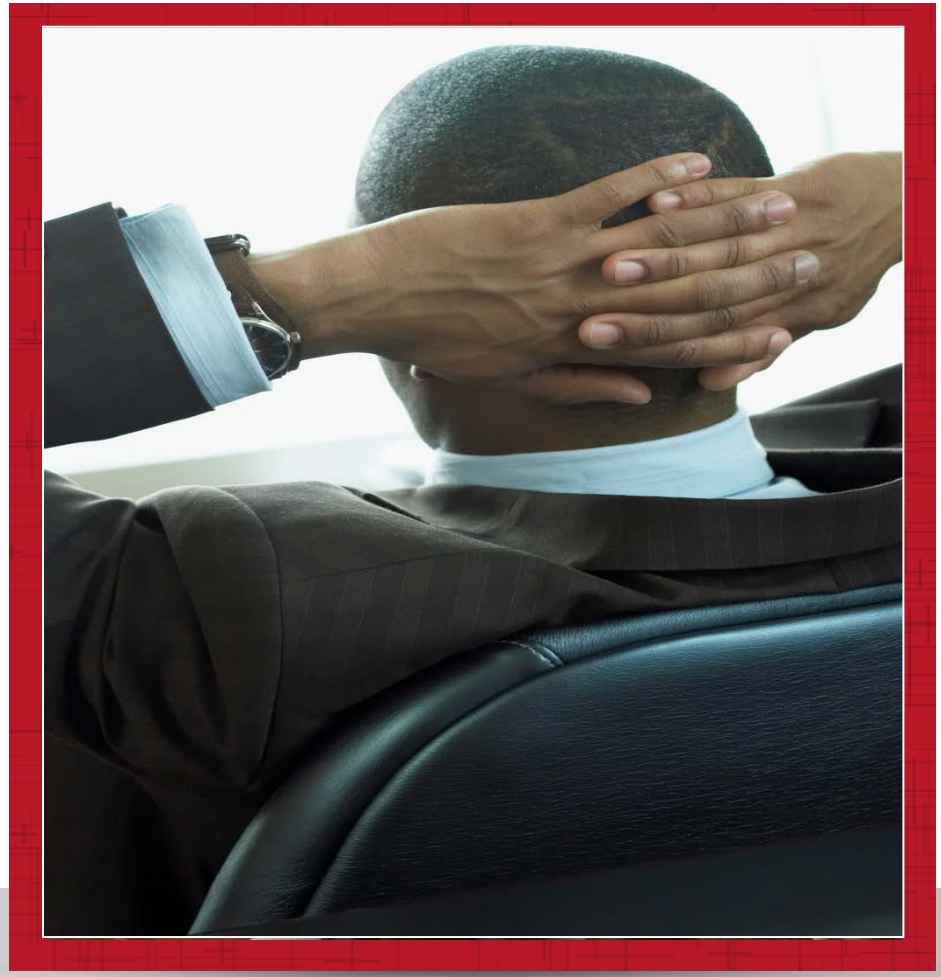
COMPLETE
VISIBILITY

FULL
ALIGNMENT

TOTAL
EFFICIENCY

McAfee's approach gets you there EASIER !

- Complete Visibility
  - Fastest path to security with complete intelligence on the location, sensitivity and vulnerability of all of your databases
- Full Alignment
  - Streamlined policy administration and protection with ZERO downtime or changes to architecture
- Total Efficiency
  - Faster time-to-compliance and lower Total Cost of Ownership



Key Solutions

Product	Description
MCAFEE VULNERABILITY MANAGER FOR DATABASES (MVM)	Discover all databases across your environment Conduct over 4,700 individual vulnerability checks across leading database systems and evaluate risk across all known threat vectors Generate detailed reports, expert recommendations for remediation
MCAFEE DATABASE ACTIVITY MONITORING	Real-time reliable protection for business-critical databases across all known threat vectors Generate detailed audit trail reports to meet compliance and audit requirements Autonomous memory-based sensor implementation effective across both physical and virtual environments
MCAFEE VIRTUAL PATCHING FOR DATABASES	Update security posture as soon as new threats are identified without downtime required by traditional patching

McAfee Vulnerability Manager for Databases

- Discover all databases that exist within your environment
- Gain insight into the security posture of each of your databases—(even the ones you didn't know about)
- Get prioritized results and expert recommendations to address vulnerabilities, saving time and cost of expensive 3rd party consultation
- Reduce time and effort preparing for and responding to compliance audits
- Manage Database Security OUTSIDE of its own silo through full integration with ePolicy Orchestrator (ePO)

"Where are all my databases, and how secure are they?"

Database Discovery and Vulnerability Assessment

BUILT ON DEEP REAL-WORLD SECURITY KNOWLEDGE

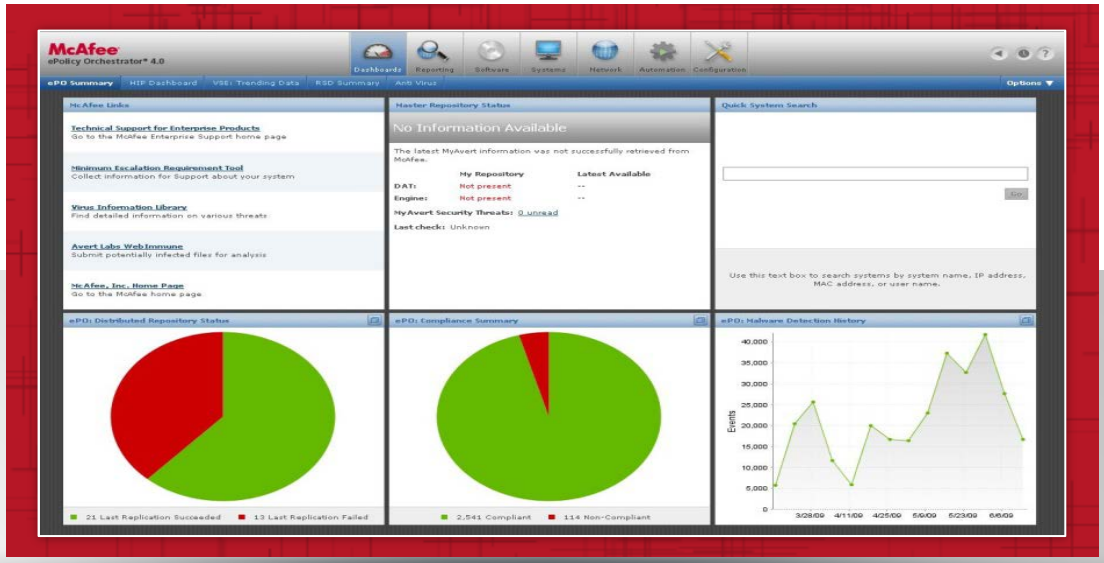
- Developed with the top authorities on database protection
- Not simply based on DBMS vendors' “security guidelines”

PROVIDE PRACTICAL REMEDY ADVICE/ SOLUTIONS

- Test and report on real issues (vs. lengthy unreadable reports)
- Prioritized results include fix scripts and expert recommendations

ENTERPRISE-READY

- Fully ePO-integrated
- Centralized reporting for up to thousands of databases
- Create different roles/outputs for various stakeholders



Most expansive set of checks Available!

McAfee
An Intel Company

Auditing

Backdoor Detection

CIS Benchmarking

DB Configuration checks

Credit Discovery

Custom checks

Data Discovery

Default Password Checks

Encryption Discovery

OS Tests

PCI DSS Checks

Password Discovery

Patch Checks

STIG Benchmarks

Unused Features

Known Vulnerabilities

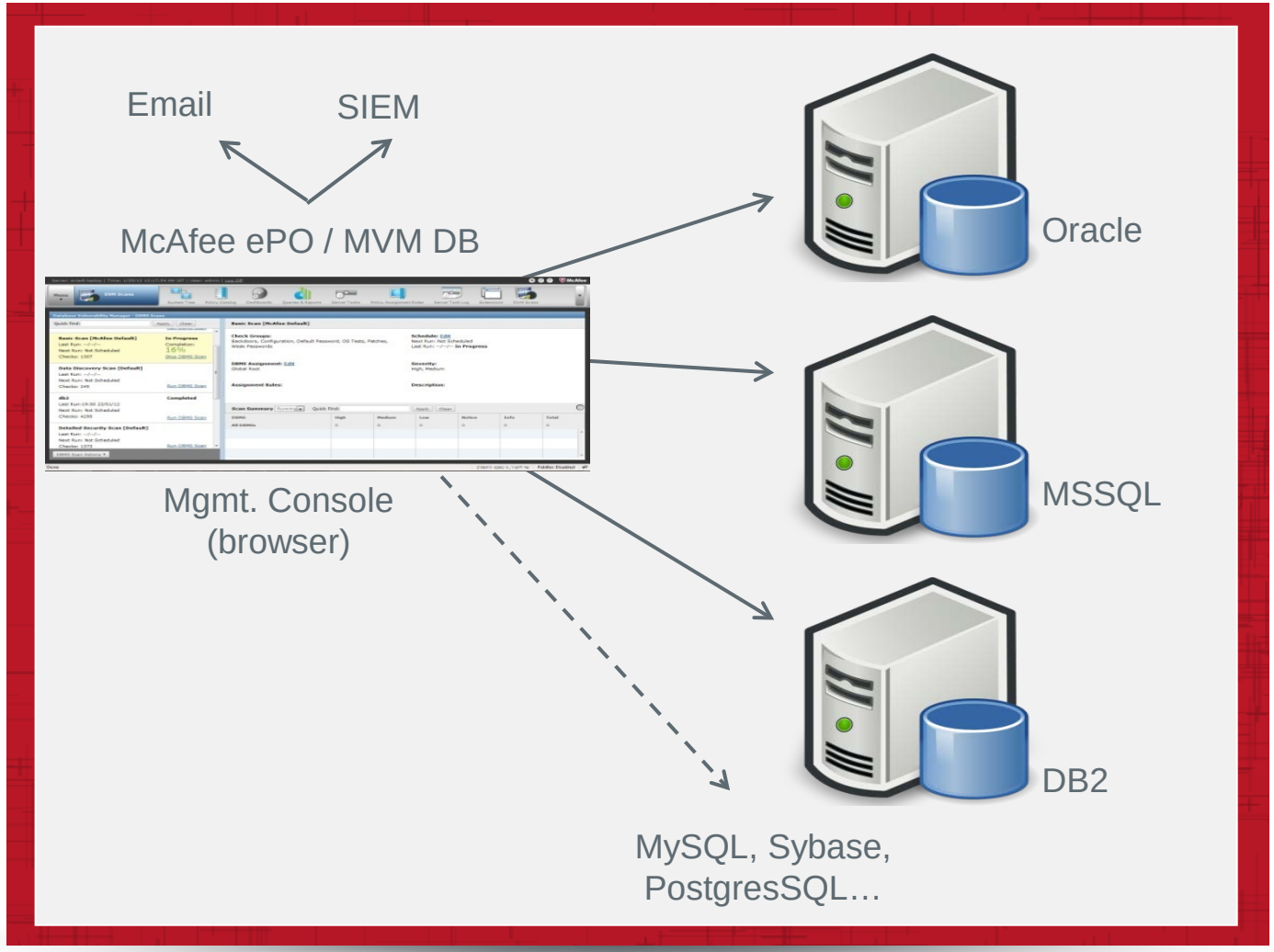
Vulnerable Code

Weak Passwords

Vulnerability Manager can perform over **4,700** individual vulnerability checks

MVM for DB — Architecture

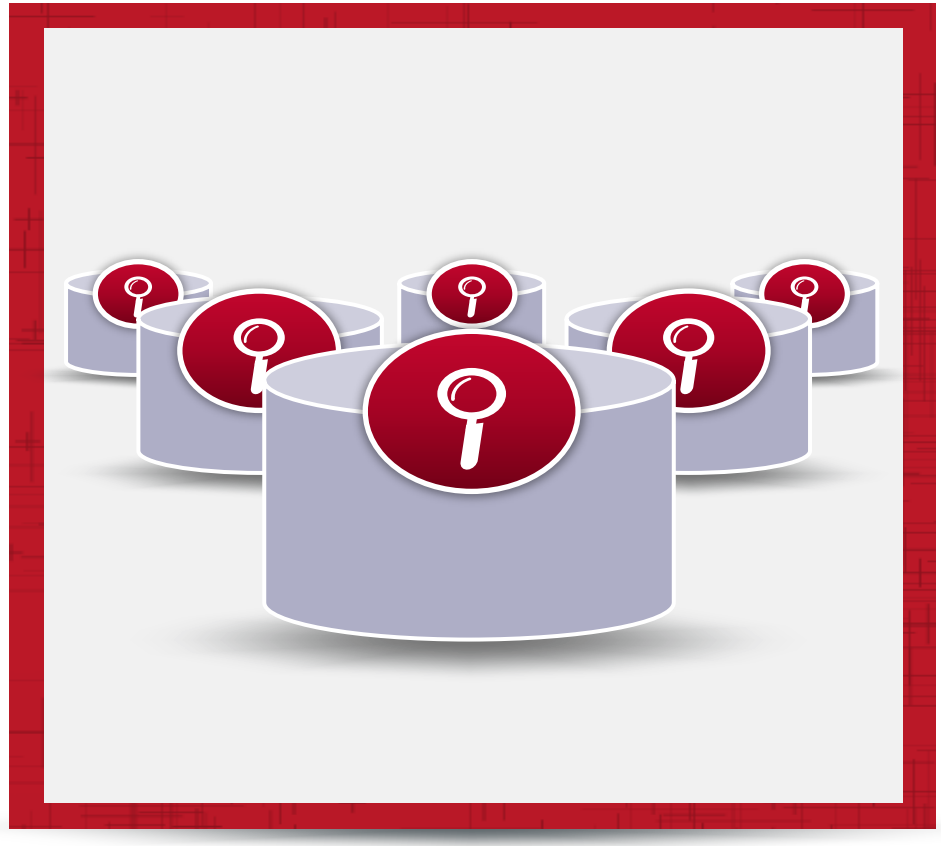
- **MVM for DB is now an extension of McAfee ePolicy Orchestrator**
  - Agent-less
  - Accessed/managed via browser
  - Performs discovery & scans over the network
  - Can scan dozens of DBs in parallel
  - Credentialed scans (read-only user)



Supported Database Platforms

McAfee Database Activity Monitoring

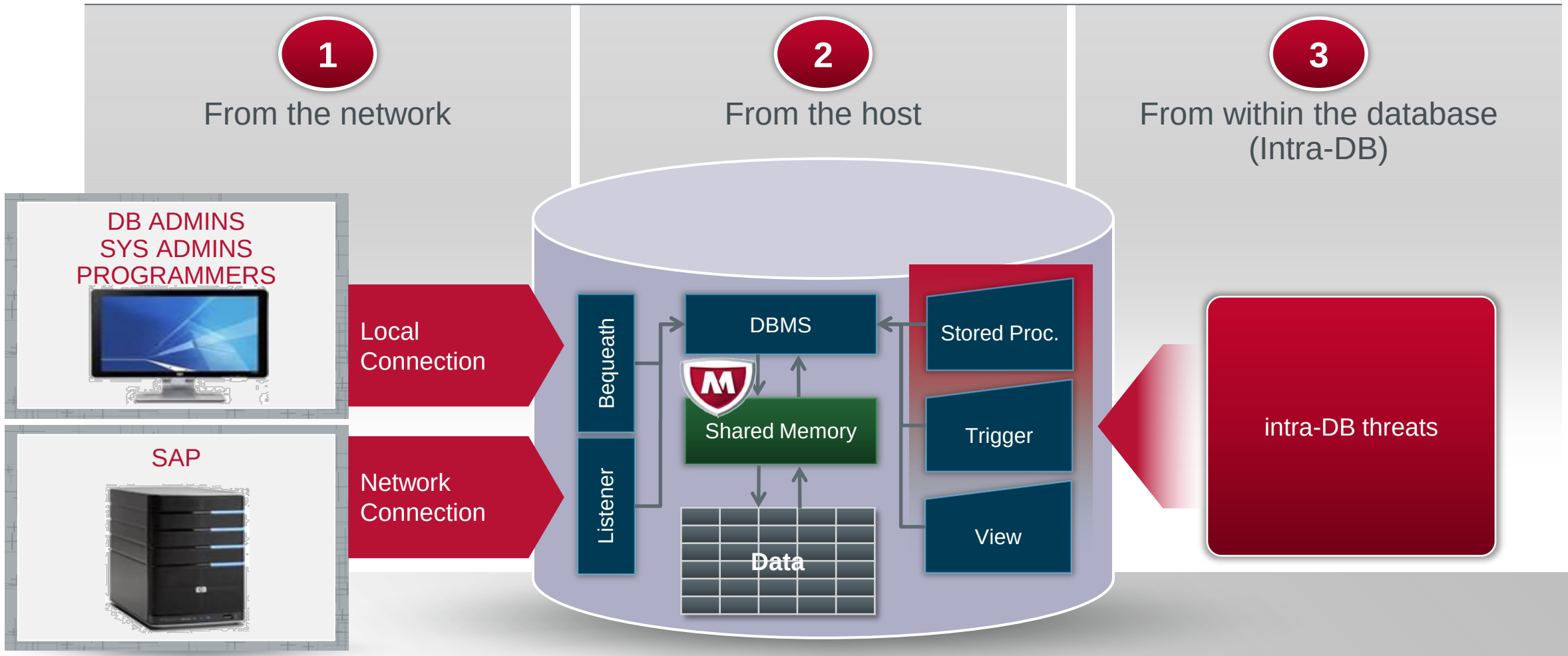
- Out-of-the-box protection for known vulnerabilities and common threats across ALL vectors
  - Real-time alerting for policy violations, even by privileged users
  - Terminates sessions and quarantines users /hosts
  - Flexible rules to reflect specific regulatory needs



"How can we protect the database AND meet compliance requirements?"

Protect the Database Across **ALL** Threat Vectors

DATABASES CAN BE ACCESSED FROM THREE SOURCES:



McAfee's Unique memory-based sensor implementation

- **Real-time database protection from the INSIDE OUT**
  - Autonomous memory-based sensors are non-intrusive
    - No changes to overall architecture needed
  - Very low impact on overall system performance (< 5%)
    Protection is easy for databases across VMs and cloud environments
- **Lower Cost and Complexity of Implementation**
  - Software-only implementation
  - Easy to download, evaluate, purchase and deploy
  - Fastest "Time-to-Compliance"

McAfee DAM uniqueness

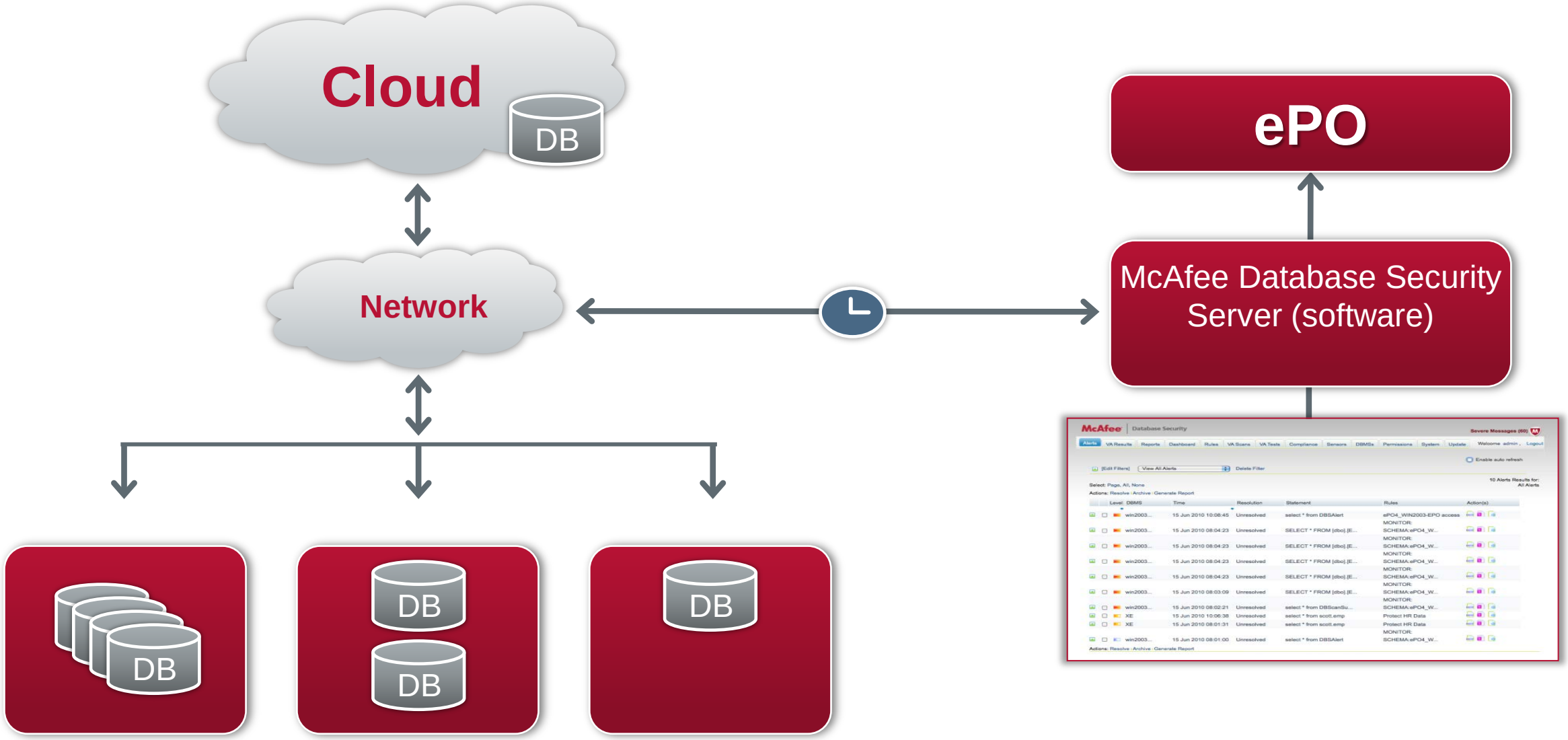
SOFTWARE-ONLY ARCHITECTURE BASED ON DB EXECUTION-PLAN

- Only one based on analyzing the DB execution-plan (as opposed to SQL sniffing at listener/bequeath/network)
- Distributed monitoring architecture, using autonomous sensors
- Decoupled from underlying physical network architecture (no SPAN/TAP ports, no mix of appliances/agents)
- Non-intrusive (no kernel/device driver)
- No in-line installation

RESULT: MOST COMPREHENSIVE AND EASIEST TO DEPLOY/USE (PARTICULARLY IN A DISTRIBUTED, DYNAMIC IT ENVIRONMENTS)

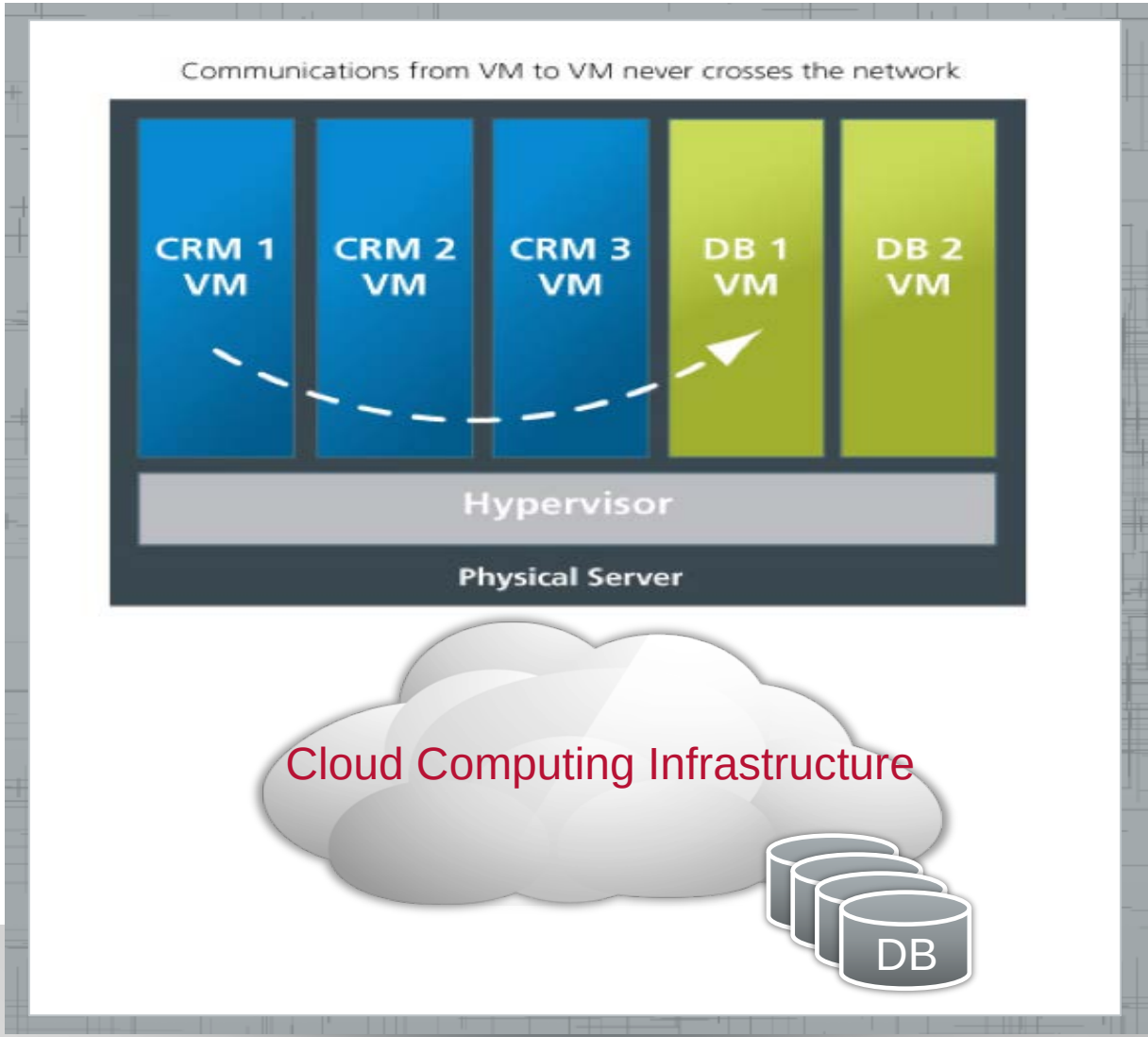
- Easily scales to VERY large environments
- Provides customers with most IT flexibility
- Operates seamlessly in VM and Cloud environments

McAfee DAM: Enterprise Deployment



Only Solution for Virtualised Environments and Cloud

- Virtualization
  - Memory-based monitoring sees VM-to-VM traffic
  - Efficient local rules processing
  - Works well in a dynamic environment
- Cloud Computing
  - Distributed model functions well even in WAN environments
  - Automated provisioning and segregation of duties allows in-house monitoring of managed services



Segregation of Duties and Audit Trail

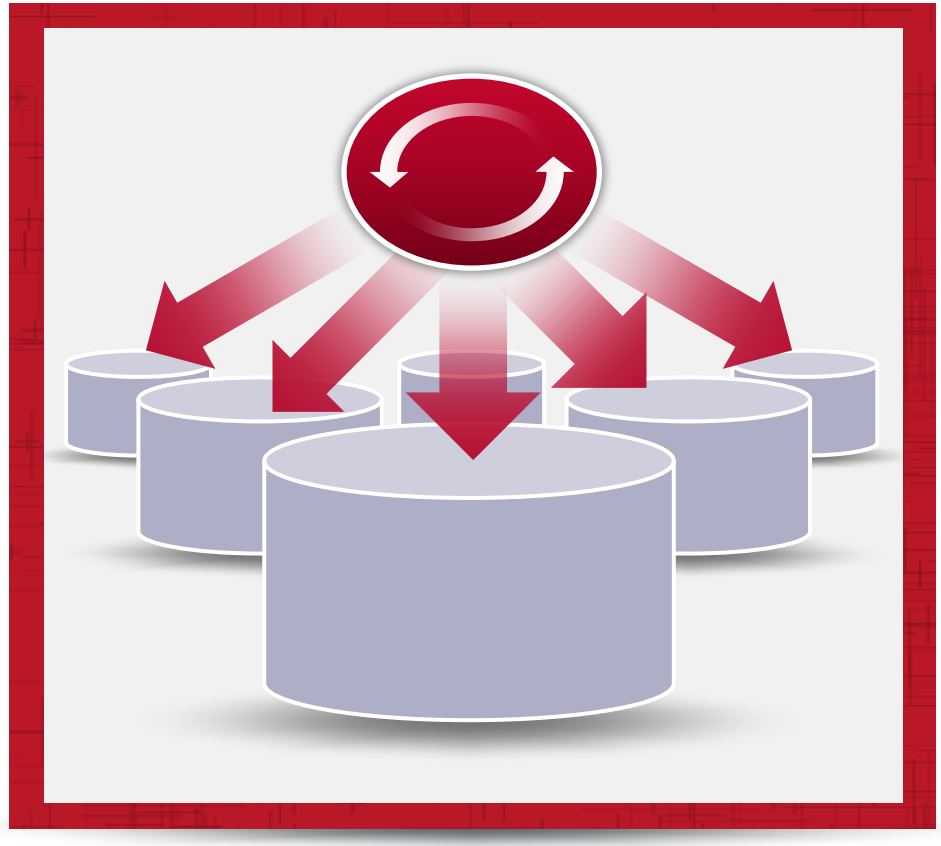
Database Administrators (DBA) and compliance team define policy

System Administrators install sensors

InfoSec monitors alerts and sensor status

McAfee Virtual Patching for Databases

- Helps achieve governance policies for patch protection with zero database downtime or disruption
- Lowers costs of development and testing by extending patch cycles and through support of older releases



"We can't keep up with all the patches for our databases, exposing us to significant security and non-compliance risk."

Unpatched Databases = Huge Risk!

EXPLOITS PUBLISHED ON THE WEB

Often do not require DBA-level skill and automated hacking tools are available

Zero Day

Reported Vulnerability

Months/Years

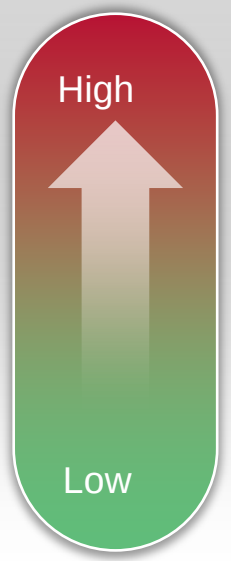
RISK IS ACTUALLY HIGHEST **AFTER** PATCH IS ISSUED

Patch Issued

Months/Years

RISK WINDOW IS OFTEN **MONTHS** LONG, SOMETIMES **YEARS**

Patch Installed



McAfee Database Security - Key Points of Differentiation

NON-INTRUSIVE IMPLEMENTATION

- Autonomous memory-based monitor implementation requires no changes to existing architecture
- Minimal impact on performance (< 5%)
- No business interruption

REAL-TIME PREVENTION ACROSS ALL THREAT VECTORS

- Memory-based monitor allows for immediate response to threats
- Virtual patching allows for immediate security updates to prevent new threats as they are profiled

IDEAL FOR VIRTUAL AND CLOUD ENVIRONMENTS

- Memory-based monitoring can see VM-to-VM traffic
- Distributed model functions well even in WAN environments

Summary - McAfee Database Security Offering

McAfee Vulnerability Manager for Databases

Extends VA capabilities to databases with over 4,300 checks for Oracle, SQL Server, DB2, MySQL, Teradata, Postgress and Sybase

McAfee Database Activity Monitoring

Unauthorized access monitoring, policy enforcement and regulatory compliance audit

McAfee vPatch

vPatch offering protects unpatched Databases against known threats, and all databases from common hacker techniques

McAfee®
An Intel Company